P 171901Z DEC 08
FM SECSTATE WASHDC
TO SECURITY OFFICER COLLECTIVE PRIORITY
AMEMBASSY TRIPOLI PRIORITY
INFO AMCONSUL CASABLANCA PRIORITY
XMT AMCONSUL JOHANNESBURG
AMCONSUL JOHANNESBURG

S E C R E T STATE 132159

NOFORN

E.O. 12958: DECL: MR
TAGS: ASEC
SUBJECT: DIPLOMATIC SECURITY DAILY

Classified By: Derived from Multiple Sources

SECRET//FGI//NOFORN//MR

Declassify on: Source marked 25X1-human, Date of source: December 16, 2008

¶1. (U) Diplomatic Security Daily, December 17, 2008

¶2. (U) Significant Events - Paragraphs 7-17

¶3. (U) Key Concerns - Paragraphs 18-29

¶4. (U) Trends and Analysis - Paragraphs 30-54

¶5. (U) Cyber Threats - Paragraphs 55-63

¶6. (U) Suspicious Activity Incidents - Paragraphs 64-82

¶7. (U) Significant Events

¶8. (SBU) EUR Belgium - RSO Brussels received a call from the U.S. Embassy's off-site mail facility personnel December 16 regarding an envelope possibly containing white powder. The mail screener noted the envelope had the same San Antonio, TX, return address as on several other envelopes sent to posts throughout Europe containing a white powder substance. The envelope was not opened; however, Post followed decontamination procedures, and the local hazmat team and Explosive Ordnance Disposal assets conducted an investigation. The facility has been sealed pending test results, and a temporary facility has been established. (RSO Brussels Spot Report)

¶9. (SBU) Germany - A U.S. Embassy Berlin local guard discovered a small package leaking a white powder placed outside the vehicle entrance to the Marine Security Guard (MSG) residence December 16. The RSO and local police determined the package originated from a pharmacy in Austria. Markings on the package, as well as a thorough examination by police, indicate the substance was known as "bitter salt," which is often used to treat an upset stomach. The RSO considers this case closed. (RSO Berlin Spot Report)

¶10. (SBU) Italy - On December 16, the Deputy Consul General called RSO Rome to report that an American Citizen Services (ACS) employee had opened an envelope which contained a suspicious piece of paper. The description of the envelope was consistent with reports of letters received by other U.S. embassies in Europe. Although witnesses reported there did not appear to be a release of white powder in the ACS office, Post took all necessary precautions. Affected employees conducted decontamination of themselves, the Consulate building and mail-handling facilities were closed pending test results, and peripherally involved employees were instructed on precautionary steps to take. (RSO Rome Spot Report)

¶11. (SBU) Romania - A U.S. Embassy Bucharest mail clerk discovered an envelope containing a white powder substance on December 16; the envelope and letter were nearly identical to

others received at European posts. The mail room was decontaminated as well as two Local Guard Force (LGF) members who were in the vicinity of the facility. The RSO sent a sample of the substance to the Centers for Disease Control and Prevention, and host-country authorities removed the letter and envelope. Post is currently awaiting the test results. (RSO Bucharest Spot Report)

¶12. (SBU) AF Democratic Republic of the Congo - RSO Kinshasa received a threatening e-mail on his DoS account from "samirmohamed2009@gmail.com" on December 16. The individual stated the U.S. Embassy lacked certain security measures and would be attacked. The RSO notified LGF and MSG assets and is investigating the incident. Apparently, before the RSO arrived at Post in August, the ARSO terminated approximately 50 LGF members for sleeping while on duty. It is possible the sender of the e-mail is a former LGF member. (RSO Kinshasa Spot Report)

¶13. (SBU) Zimbabwe - Emergency Action Committee (EAC) Harare convened December 15 to review trip wires relevant to the cholera epidemic in-country and the collapse of medical services. EAC members agreed the situation falls within the "Growing Potential for Drawdown" category in which the U.S. Embassy has operated in since March 2007. The EAC reviewed existing precautions and recommended others, including funding to purchase an additional water truck and water purification unit. (Harare 1125)

¶14. (S) NEA Libya - An unidentified individual called U.S. Embassy Tripoli December 15 with possible threat information. The caller stated his son was planning to leave Libya to "do jihad against the Americans." The caller refused to identify himself or his son, and would not provide his telephone number. The caller stated he would call back in a day to provide more information; however, he has not called Post again. (Appendix source 1)

¶15. (SBU) EAP The Philippines - EAC Manila convened to discuss the U.S. Embassy's holiday security posture. The RSO briefed on the security situation, and EAC members agreed Post's current security measures are appropriate. (Manila 2728)

¶16. (SBU) SCA Pakistan - U.S. Consulate Peshawar personnel heard/felt a large explosion December 16 at 9:15 a.m. Regional Security Office sources quickly confirmed that a suspected 107 mm rocket impacted a residence in the civil quarter's section of the Peshawar military cantonment, which is located approximately 850 meters east of the Consulate facilities. Two local nationals were injured in the attack. (RSO Peshawar Spot Report)

¶17. (SBU) Domestic Massachusetts - Boston Field Office (BFO) agents and Boston Police Department (BPD) officers monitored a demonstration of 15 to 20 members of the Boston Anti-Authoritarian Movement (BAAM), a local anarchist group, on December 16 at the Greek Consulate. After the agents and law enforcement officers departed the scene, five individuals attempted to force their way past a security guard and caused minor damage to the external gate of the consulate. The BPD is conducting an investigation of the incident. (BFO Spot Report)

¶18. (U) Key Concerns

¶19. (S//NF) EUR Georgia - Abkhaz border region may see renewed fighting: Ten tanks bearing Abkhaz flags were seen traveling southeast from Gali, Abkhazia, toward the Georgian border along the main highway yesterday, December 16. This movement comes just one day after Russian military equipment was noted withdrawing from the vicinity, and at least 33 Abkhaz tanks were spotted in the frontier area of Ganmukhuri. The movements likely signify an upcoming Abkhaz offensive on the last remaining Georgian territory north of the Inguri River is a distinct short-term possibility, since the lack of Russian military in the area will allow the Russian peacekeepers plausible deniability for the attack. Prior to

open hostilities this summer, Gali was a predominantly ethnic-Georgian town just north of the Abkhaz-Georgian demarcation line; however, fighting forced the Georgians several miles to the south, into Georgian territory. Reporting indicates the Georgian military may be preparing for a potential clash, as high-performance jet aircraft were heard circling over the city of Zugdidi, just over the demarcation line from Gali, repeatedly late Monday (December 15) evening. (Appendix sources 2-3)

¶20. (S//NF) NEA Lebanon - Drug trafficking organization possibly intending to kidnap Americans: Sensitive reporting alleges Noah Zeiter, a Lebanon-based drug lord, intends to kidnap AmCits in Lebanon if his brother receives a proposed 20-year prison sentence in the United States.

¶21. (S//NF) DS/TIA/ITA notes Noah Zeiter (variant: Nouh Zaayter) is the head of the Zeiter Drug Trafficking Organization (DTO) who allegedly has ties to officials affiliated with Lebanese Hizballah. The Zeiter organization is the most infamous of about 50 fiercely independent tribal-based drug-trafficking organizations that operate with near impunity in Lebanon's northern Bekaa Valley. Even Hizballah, who exerts significant political, economic, and military influence in the region, is hesitant to confront these powerful groups, many of whom also operate outside the authority of the Lebanese Government. The Zeiter DTO allegedly facilitates the transportation of cocaine from South America to the Middle East and Europe, and oversees the production of cannabis in Lebanon.

¶22. (S//NF) Noah Zeiter's brother, Yehya Zeiter, was arrested in Romania in August on drug-related charges and is scheduled to be extradited to the United States (NFI). Given Noah Zeiter's extensive criminal history and disregard for authority, it is certainly possible members of his organization, or criminals or extremists hired by him, could lash out at the U.S. by attempting to kidnap or harm AmCits in Lebanon if his brother is sentenced to a lengthy prison term in the United States. An October 4 Agence France-Presse article reported Noah Zeiter is wanted on 487 criminal charges including drug trafficking, kidnapping, car theft, terrorism, weapons dealing, fraud, and extortion. DS/TIA/ITA will continue to monitor this situation and provide warning if and when Yehya Zeiter is sentenced. (Appendix source 4)

¶23. (S//NF) EAP Indonesia - Alleged Christmas day attack planned: According to recent intelligence information, Jemaah Islamiyah (JI) -- a transnational Southeast Asian terrorist group with connections to al-Qa'ida -- and other Islamic extremist groups allegedly are planning to transport explosives from West Sumatra to Jakarta for Christmas day attacks. The information was received thirdhand, originating with an ultimate subsource who claimed to be a JI member in West Sumatra. The report alleges, as of mid-December, senior JI figure Abu Tholut planned to travel to Lampung, West Sumatra, between December 19 and 21 for the purpose of facilitating the shipment of explosive material to Jakarta to be used in unspecified Christmas day attacks.

¶24. (S//NF) The report further discusses the subsource's alleged mid-December meeting with members of a Lampung JI cell traveling through Jakarta; Tholut requested members of the cell accompany him back to Lampung to assist in his efforts. Tholut also boasted to the cell members that he had received 700 million Indonesian rupiah to assist with Christmas season operations; Tholut did not reveal the source of the funds. (Comment: 700 million Indonesian rupiah equals approximately $64,000 at a mid-December exchange rate of Indonesian 11,000 rupiah/U.S. dollar.) Tholut sought the assistance of these particular cell members because some were veterans of Afghan fighting with expertise in explosives. One of the cell members, Ustadz Marzuki (Terrorist Identities Datamart Environment (TIDE) number 170584), agreed to travel with Tholut. Marzuki is reportedly a JI member who was arrested in July 2003 (released August 2003 due to lack of evidence) for possible involvement with the April 2003 bomb that detonated at Soekarno-Hatta Airport in Jakarta.

¶25. (S//NF) DS/TIA/ITA notes, as of early December, multiple collateral reports indicate Abu Tholut (TIDE number 125518), ostensibly a senior member of JI, was arrested and sentenced to seven years of imprisonment in July 2003 for possession and hiding of explosives and weapons in Semarang and Jakarta. Although Tholut was cleared of terrorism charges, he is currently not due for release until 2011.

¶26. (S//NF) DS/TIA/ITA notes the information contained in this report hinges on the assumption that Tholut has been released from prison and is currently in circulation; although, collateral sensitive reports refute this possibility. DS/TIA/ITA further notes this threat report lacks specifics and thorough vetting, and involves a lengthy chain of acquisition. JI has attacked during this time period in the past when on Christmas Eve 2000, JI was responsible for multiple bombings. These incidents -- some 20 in all -- claimed the lives of 19 people and injured 47 in Jakarta and five other Indonesian cities. (Appendix source 5)

¶27. (S//NF) SCA Pakistan - Taliban plans to participate in attacks in Quetta, possibly Karachi: As of early December, Abdul Bari, former deputy of the deceased Maulawi Aminullah, met with several Taliban commanders for Qandahar and Oruzgan provinces to apprise them of Taliban plans for Afghanistan and Pakistan, according to a developing source claiming firsthand access. Bari stated the Taliban planned to participate in upcoming unspecified attacks in Quetta and greater Baluchistan Province, including possible activity in Karachi, Sindh Province. Bari warned the operations would be more damaging than unspecified attacks in Peshawar and Islamabad. Bari further noted the Taliban would suspend most of its operations in Afghanistan during the winter months due to expectations of harsh weather conditions and to allow Mullah Salam to transition into Maulawi Aminullah's now vacant position as an expert on improvised explosive devices (IEDs).

¶28. (S//NF) DS/TIA/ITA notes earlier reporting suggests Taliban leaders of the Quetta shura are increasingly concerned for their security following arrests of their cohorts in the city by Pakistani security officials earlier this year and have increasingly relied on Karachi as a secondary hub. It is plausible Abdul Bari (TIDE number 44480), a Taliban subcommander reportedly working at a training center southwest of Quetta, is referencing plans by the Pakistani Taliban Movement and its foreign affiliates to carry out terrorist attacks in Baluchistan, primarily targeting the Frontier Corps and then local law enforcement first reporting by Pakistan's Inter-Services Intelligence (ISI) in mid-October. Extremists also reportedly expressed interest in kidnapping an ISI officer, U.S. officials, and U.S. Citizens. Pakistani authorities assessed the strategy of broadening the terrorist campaign to Baluchistan resulted from increased activity by Pakistani military elements against terrorists in Baluchistan and elsewhere. Separately, however, there are few indications Taliban operations in Afghanistan will slow during the forthcoming winter.

¶29. (S//NF) On September 24, a suicide operative carrying 10 kg of explosives targeted a Frontier Corps vehicle in Quetta, killing one and injuring 22. Pakistani press reports also detail the July 22 seizure of a vehicle carrying explosives and four alleged suicide operatives. On December 15, 2007, dual suicide blasts killed at least eight people, including a number of security personnel at a checkpoint near a high-security military cantonment in the Kachh Mor area of Quetta, Baluchistan, on December 13. The second bomber apparently targeted first-responders and bystanders congregating at the primary blast scene. (Appendix sources 6-8)

¶30. (U) Threats & Analysis

¶31. (S//NF) AF Niger - Two tearlines from December 16 suggest al-Qa'ida in the Lands of the Islamic Maghreb's (AQIM's) complicity in the December 15 kidnapping of a UN special

envoy to Niger and Canadian Ambassador Robert Fowler (and his special assistant, Louis Guay). Tearline from December 16 reads, "Two Canadians taken hostage in Niger were possibly transported to AQIM in Mali on December 15. Mali-based AQIM leader Mokhtar Belmokhtar's associate Hamed may have received the hostages from a Tuareg in Mali near the Mali-Niger border. Hamed later began travel north to meet Belmokhtar."

¶32. (S) Earlier tearline from the same day stated, "Nigerien Movement for Justice (MNJ) and Front for Redress Forces (FFR) reportedly were not involved in the mid-December kidnapping of a Canadian citizen. However, a Tuareg associate of AQIM may have been involved. The Tuareg was in the same region as the Canadian during the time frame he was apparently kidnapped. Following the kidnapping, the Tuareg traveled to Mali where he apparently met with an associate of AQIM el-Moulethamine battalion leader Mokhtar Belmokhtar near the Niger-Mali border. Belmokhtar's associate then returned to Belmokhtar's location approximately 250 km west of Kidal, Mali."

¶33. (S//NF) DS/TIA/ITA cannot immediately substantiate that AQIM is indeed holding the hostages, but previous reporting has highlighted the group's and Belmokhtar's intent to conduct kidnapping operations. Additionally, the recent ransom payment AQIM received for the Austrian hostages may have emboldened nefarious and AQIM-aligned elements in the region to conduct this operation. After the Austrian hostages were released in northern Mali on October 3, Abdousalam Ag Assalat, a member of the Tuareg rebel movement Alliance for Democracy and Change, told U.S. Embassy Bamako AQIM had offered a bounty of approximately $45,000 to any traffickers and bandits in northern Mali who kidnapped non-American Westerners. Also of note, Belmokhtar allegedly tasked operatives on several occasions with kidnapping-for-ransom operations, including an abduction operation targeting the German deputy chief of mission in Nouakchott, Mauritania. Concurrently, Belmokhtar has also specifically ordered his operatives to avoid targeting Am
Cits for fear of retribution from the government.

¶34. (S//NF) Although many of the details of this specific operation remain unclear, it was likely an ad-hoc operation and a target of opportunity, possibly in response to the bounty offered by AQIM. According to U.S. Embassy Niamey reporting, the kidnapping occurred after Ambassador Fowler journeyed to a gold mine located in the southwest city of Tera on December 14. The incident itself occurred in the Tillabeyi region of Niger, approximately 40 km from the capital, and the site of 2008's Niger Republic Day festivities; last year's celebrations in northern Tahou witnessed a land mine explosion.

¶35. (S//NF) The trip was described as personal business, and he did not coordinate the trip with the Nigerien authorities, the UN, or the Canadian Embassy. After visiting the mine, Fowler and Guay contacted the Canadian chief of mission (COM) at 4:40 p.m. At the time, they were located at the ferry crossing and were expected back in Niamey at approximately 7:30 p.m. After Guay failed to show up for dinner with the Canadian COM in Niamey that evening, local police began searching for both Fowler and Guay. In the early morning of December 15, the police discovered their abandoned UN vehicle -- which was unmarked aside from UN license plates -- parked on the right side of the road with the motor running and a turn signal blinking. Nothing was taken from the vehicle.

¶36. (S//NF) Initial speculation as to the culprits centered on the FFR. On early December 15, they issued a claim of responsibility on their website, stating Ambassador Fowler was safe and would be moved to another location where he would be transferred to unidentified collaborators. They also cited the kidnapping as a warning to all diplomats who allegedly collaborate with the "ethnocidal regime" of Nigerien President Mamadou Tandja. The statement was signed by FFR leader Rhissa Ag Boula. A follow-up website statement by Mohamed Aquitcki Kriska, the president of FFR, denied the group had conducted the hostage operation. U.S. Embassy

Niamey also questioned the veracity of Ag Boula's statement due to inaccuracies in the timing of the event and the number of hostages taken. DS/TIA/ITA notes it is unlikely either the MNJ or FFR sanctioned this kidnapping operation, as they both have a historically contentious relationship with AQIM. They also do not operate in southwestern Niger, where Fowler was allegedly kidnapped. Instead, they are largely confined to their indigenous lands in the north.

¶37. (S//NF) The kidnapping may also have wider strategic implications for neighboring countries. If AQIM keeps the hostages in northern Mali, as it did with the Austrian hostages for nearly eight months, the Malian Government will likely face strong international pressure to increase its counterterrorism operations against the group and to ignore an unwritten deal that AQIM will not attack in Mali if the government does not crack down on the group's operations in the region. (Open sources; Niamey 0572; Appendix sources 9-30)

¶38. (S//FGI//NF) SCA India - Review of LT commanders involved in Mumbai attacks: Following the reported Pakistani detentions of Lashkar-e-Tayyiba (LT) operational commander Zaki-ur Rehman Lakhvi (TIDE number 117632), LT communications coordinator Zarrar Sha (variant: Shar or Dar; TIDE number 19972343), and LT founder and leader Hafiz Saeed (TIDE number 68897), Bangladeshi security forces detained LT operatives Yahya (a.k.a. Mubashir Shahid; TIDE number 21577558) as he attempted to board a Pakistani Airlines flight from Dhaka to Karachi on December 8. These operatives, among others, are operationally linked to the late-November three-day armed siege of Mumbai. While their detentions are welcome developments, a number of other LT operatives also linked to Mumbai remain at large, including Rana Rehan (a.k.a. Abdul Aziz; TIDE number 20876466), Yusuf Muzamil (TIDE number 23283695), Kaffa (TIDE number 23329151), and Azam Cheema (TIDE number 19924808). With these experienced organizational and training commanders still free, the potential for additional attacks to be coordinated and executed in Kashmir and mainland India by this network remains.

¶39. (S//FGI//NF) LT's Pakistan recruiting and training network remains a primary concern in gauging the lethality of future operations, as demonstrated by the effective tactics and techniques used by the LT gunmen in the siege of Mumbai. Azam Cheema, LT's chief commander for cross-border operations and head of the network's training programs, is currently based in Pakistan and likely played a critical role in coordinating the most recent Mumbai attack. Worryingly, Cheema is suspected of playing a key role in the Mumbai train blasts on July 11, 2006, as well. Although Pakistan's ISI detained Cheema in March 2007, he was released a few months later in June, after which he relayed the ISI orchestrated his detention for his own safety, according to a sensitive source with access. Such precedents indeed bring into question the sustainability of recent Pakistani efforts to crack down on LT's infrastructure within the country.

¶40. (S//FGI//NF) LT commanders with experience to operate regionally are also of concern. Available reporting suggests Muzamil, his assistant Kaffa, and Rehan played key roles in organizing the Mumbai attacks and are particularly savvy in the establishment and management of LT's network in third-party countries, namely the United Arab Emirates, Bangladesh, and Nepal, for illicit funding and procurement activities. Muzamil, who reportedly directed the Mumbai attacks in concert with the now-detained Lakhvi, relied on Rana Rehan as his deputy for LT's mainland India operations. Rehan directly managed Yahya in Bangladesh, who ran at least three front companies for LT in the country. Likewise, Rehan also reportedly established LT's footprint in Nepal. This regional network has been actively targeting India for at least three years; a review of earlier reporting further indicates Muzamil, Rehan, and Yahya also worked with the now-deceased Shahid Bilal (TIDE number 11009529; a Bangladeshi Islamist with ties to LT), whose network executed attacks on the mainland since 2005.

¶41. (S//FGI//NF) A review of past attacks orchestrated by LT

and its regional affiliates suggests LT is likely capable of conducting another attack in India in the coming months; although, it remains unclear what such an operation would target. In mainland India, LT has conducted approximately three or four operations per year (see chronology below). Indeed, India remains concerned of the possibility of an additional attack by LT or another extremist group. Tearline notes, "On December 15, India contacted the Heads of Mission of Indian embassies with a terrorist alert. It warned that, according to information received, Pakistan-based terrorist groups, emboldened by the publicity surround the Mumbai attacks, may target Indian missions in Colombo, Dhaka, Kathmandu, Nairobi, Dar Es Salaam, and Addis Ababa, besides attempting other dramatic terror strikes (sic). Security measures were to be strengthened." Similarly, tearline from early December reported, "LT terrorists may be planning attacks against civilian infrastructure sites in the states of Jammu and Kashmir. Possible attack locations include several dams, power stations, and three airports -- Leh Airport, Kargil Airport, and Jammu Satwari Airport."

¶42. (SBU) Recent attacks linked to LT and/or the Shahid Bilal network:

¶43. (SBU) November 26 to 29 - Mumbai, Karnataka (southwest India): At least 10 LT assailants execute an extended armed assault that leaves nearly 200 dead, including 22 foreigners. The gunmen attack various locales in the well-to-do Colaba-Nariman point area, including the Taj Mahal Hotel, the Trident/Oberoi Hotel, the main train station, and a Jewish center.

¶44. (S//NF) August 25, 2007 - Hyderabad, Andhra Pradesh (south-central India): Bilal's network of militants is suspected of carrying out twin bombings.

¶45. (S//NF) May 18, 2007 - Hyderabad, Andhra Pradesh: The Shahid Bilal network carries out the Mecca Mosque blast that kills 11 people.

¶46. (SBU) February 19, 2007 - Dewana, Haryana (northern India): The "Friendship Train" between India and Pakistan is bombed, killing 68 and injuring 12, most of whom were Pakistani nationals.

¶47. (SBU) September 8, 2006 - Malegaon, Maharashtra (western India): LT members target a mosque with a timed IED, killing 37 and injuring 100.

¶48. (SBU) July 11, 2006 - Mumbai, Karnataka: Commuter trains are hit by timed IEDs, killing 170 and injuring 450.

¶49. (SBU) April 14, 2006 - New Delhi, Delhi (northern India): Seventeen people are injured when a small bomb explodes after Friday evening prayers at the crowded 17th-century Jama Masjid in the old quarter of the capital.

¶50. (S//NF) March 7, 2006 - Varanasi, Uttar Pradesh (northern India): Bilal operatives attack a prominent Hindu shrine, killing 20 and injuring 60.

¶51. (SBU) December 28, 2005 - Bangalore, Karnataka: Gunmen attack the Indian Institute of Science, killing one and injuring five.

¶52. (SBU) October 29, 2005 - New Delhi, Delhi: Timed bomb blasts hit a marketplace, killing 66 and injuring 200.

¶53. (SBU) October 12, 2005 - Hyderabad, Andhra Pradesh (northern India): The Police Task Force Command headquarters is attacked by a suicide bomber, killing one and injuring one.

¶54. (S//NF) July 28, 2005 - Jaunpur, Uttar Pradesh: The Bilal network attacks the Shramjivi Express train, killing 13 and injuring 50. (Appendix sources 31-43)

¶55. (U) Cyber Threats

¶56. (U) Worldwide - Media connects IMF attacks to the PRC:

¶57. (SBU) Key highlights:
o IMF computers have been subjected to a major data breach.
o Several observers have linked the IMF and WBG attacks to the PRC.
o Open source linkages to the PRC are speculative and not based on evidence.
o It is possible this activity is related to any number of worldwide actors.

¶58. (U) Source paragraph: "The discovery of the assault last week threw into crisis the Washington, DC-based International Monetary Fund (IMF), which offers emergency financial aid to countries faced with balance-of-payments problems, and provoked a shutdown of IMF computers that lasted for several days."

¶59. (U) CTAD comment: Media reports claim computers belonging to the IMF have undergone a serious data breach. According to Fox News, the organization was subjected to a critical intrusion just weeks after a series of attacks took place against its sister organization, the World Bank Group (WBG). The organizations have denied the specifics of the news reports, and many observers believe the People's Republic of China (PRC) is responsible for the attacks.

¶60. (U) CTAD comment: In October, Fox News reported that several intrusions against the WBG had occurred since September 2007, when intruders allegedly targeted a data store in Johannesburg, South Africa. The news agency also claims the WBG came under attack again from the same Chinese Internet Protocol range between June and July. As proof, the media outlet produced an internal memo -- supposedly verified by a World Bank spokesman to another news outlet -- stating at least five servers containing sensitive data had been compromised. Additionally, workers from an Indian information technology contractor were implicated in the installation of keystroke-logging software on WBG computers (see CTAD Daily Read File (DRF) dated October 17). In the wake of the October report, Fox News claims the WBG is now changing computer systems.

¶61. (U) CTAD comment: Most recently, Fox News is claiming the IMF also has become the victim of a related intrusion, which may have accidentally migrated from WBG computers after an office move. According to sources cited by the news agency, the IMF locked down its networks on November 7, days after the WBG moved more than 100 of its employees onto a floor in a Washington, DC, office belonging to the IMF. Fox has speculated the networks, which were previously separated by a firewall, may have become cross-contaminated after the move. For its part, the IMF has denied that any lockdown took place; although, it acknowledges severing its connection with the WBG and implementing enhanced security measures.

¶62. (U) CTAD comment: Speculation regarding the source of the attacks has widely implicated the PRC, whom many commentators assert has the desire and the demonstrated ability to obtain sensitive IMF and WBG information. Open source reporting quotes former U.S. intelligence personnel who insinuate the attacks are most likely the work of the PRC, but only establish links based on the volume of PRC computer network operations (CNO). Other reporting discusses possible PRC motivations and establishes linkages based on the value IMF and WBG information would have to the country.

¶63. (S//NF) CTAD comment: Byzantine Hades, a series of related computer-network intrusions with a believed nexus to the PRC, has affected U.S. and foreign government systems as well as those systems belonging to international organizations, such as human rights organizations (see CTAD DRF dated May 28). The intrusion set has collected intelligence of varying importance, to include the type of economic information that would be housed in IMF and WBG networks. It is reasonable to assume the PRC has the motive and ability to perpetrate attacks on those networks; however, no evidence has yet supported this conclusion. It is also

possible that the computer intrusions were the result of indiscriminate computer crime. Furthermore, there are several nations that have the ability to conduct CNO targeting the IMF and WBG, and virtually every country has a motive to collect intelligence on those organizations, given the major geopolitical ramifications of IMF and WBG activities. The absence of any available evidence at
this time makes it premature to implicate any actor for these intrusions. (FoxNews.com (www.foxnews.com), "Cyber-Hackers Break Into IMF Computer System," November 14, 2008; Appendix source 44)

¶64. (U) Suspicious Activity Incidents

¶65. (SBU) WHA Nicaragua - Surveillance Detection Team (SDT) Managua observed a vehicle with four occupants in a parking lot near the U.S. Embassy December 11. Local police interviewed the occupants, who stated they were supposed to meet someone there. After approximately 15 minutes, the vehicle departed the area; the occupants did not meet anyone.

¶66. (SBU) Record Check/Investigation: Driver: Humberto Alberto Melgar Medina. Vehicle: Black Toyota Echo (four door); License plate: P111 447 (El Salvador). (SIMAS Event: Managua-00822-2008)

¶67. (SBU) EUR Turkey - On November 10, a man approached the U.S. Embassy Ankara intercom and indicated he wanted to talk to an Embassy officer. The subject said he was an Iranian citizen highly "demoralized" because his application for asylum as a refugee was rejected by the UN. He held up a plastic bag containing stones to the Embassy camera and said he wanted to throw the stones at Post if there is nobody available at the compound. Police were notified and detained the subject. They obtained his biographical data and released him.

¶68. (SBU) Record Check/Investigation: Subject: Aliakbar Ebrahimi. DPOB: 1977; Tehran, Iran. (SIMAS Event: Ankara-00427-2008)

¶69. (SBU) NEA Jordan - A suspicious vehicle with two occupants stopped approximately 50 meters from U.S. Embassy Amman November 16. One of the occupants asked (unknowingly) an SDT member if he works in the area and asked twice about American facilities in the area. When the SDT member did not answer, the pair departed the area. Further information will be reported as it becomes available.

¶70. (SBU) Record Check/Investigation: Vehicle: Silver Daewoo Nubira; License plate: 15-65498. (SIMAS Event: Amman-03499-2008)

¶71. (SBU) Tunisia - A vehicle with two men drove back and forth in front of U.S. Embassy Tunis December 9 and stopped in Post's parking lot. The passenger exited the car and presented his Libyan passport to the guard to apply for a visa. The subject was told the Embassy was closed. Fifteen minutes later, the subjects drove away.

¶72. (SBU) RSO Action/Assessment: It is not uncommon for Libyans to drive to Tunis to submit their visa applications, as Consular services are limited in Tripoli, Libya. Also, first-time visitors to Post are often confused on the parking situation, especially at the Consular Section. This is noteworthy because the applicant did not have an appointment. (SIMAS Event: Tunis-01892-2008)

¶73. (SBU) EAP Brunei Darussalam - SDT Bandar Seri Begawan observed a man near the building housing the U.S. Embassy on December 12. He acted in a suspicious manner and took photographs. Local police interviewed the subject, who stated he is a private investigator and previously a Brunei police officer.

¶74. (SBU) RSO Action/Assessment: The Regional Security Office was unable to verify the subject's employment. His biographical information was passed to the Brunei Internal

Security Department to determine if he is a licensed private investigator.

¶75. (SBU) Record Check/Investigation: Subject: Abdul Hamid Hamli. DOB: June 9, 1946. (SIMAS Event: Bandar Seri Begawan-00202-2008)

¶76. (SBU) SCA India - SDT Mumbai observed a vehicle crash into the perimeter fence of the New Consulate Compound in Mumbai December 11. The vehicle did not enter the compound, and there were no injuries. According to LGF personnel, the driver was traveling at high rate of speed and lost control of the vehicle while making a turn.

¶77. (SBU) Record Check/Investigation: Subject: Rajesh Tanavari. DOB: March 1, 1973. (SIMAS Event: Mumbai-00317-2008)

¶78. (SBU) Nepal - LGF Kathmandu observed a man photographing the main compound access control area of the U.S. Embassy December 7. Local police questioned the subject, who stated he was a Nepalese Army officer and was photographing various diplomatic offices for security purposes. The man was released after his biographical information was obtained.

¶79. (SBU) RSO Action/Assessment: The Regional Security Office forwarded this information to the Defense Attach Office for verification with the Nepalese military. The RSO was informed by Australian Embassy personnel that a similar event had occurred at their compound the next day.

¶80. (SBU) Record Check/Investigation: Subject: Bikram Thapa. DOB: August 20, 1983. (SIMAS Event: Kathmandu-02260-2008)

¶81. (SBU) Tajikistan - A man carrying a bag approached the U.S. Embassy Dushanbe pedestrian gate December 12 at 1:40 p.m. and asked to speak with the main person of the Embassy. The man stated he had problems and came to Post, as it was his last chance to solve them. He then became excited and stated he had a bomb in his bag and should be arrested. LGF personnel smelled alcohol on the subject's breath and called the Regional Security Office. Local police were notified, and a K-9 dog checked the man and his bag with negative results. Itemizer swipes were also taken of the man and his bag, which returned positive hits for TNT and RDX. Police took the man into custody.

¶82. (SBU) Record Check/Investigation: Subject: Vladimir Anatolievich Kirtkoev. DOB: March 12, 1977. (SIMAS Event: Dushanbe-0277-2008)

SECRET//FGI//NOFORN//MR

Full Appendix with sourcing available upon request.

RICE